# The dangers of encryption

Chris Mitchell

Nowadays there is a plethora of products designed to enable PC users to encrypt sensitive data. Probably the most well known of them is PGP, but there are many others. Some come as part of larger PKI-based packages designed for corporate use, whereas others are aimed at the home user. All these products are designed to protect the confidentiality of stored or transmitted data, and we are often actively encouraged to use these products to make our PCs more secure. However, life is not always so simple.

All encryption products use cryptographic keys. These keys play a critical role – without the right key, decryption is not possible. This is both necessary for security – otherwise, anyone with the same product could decrypt all your encrypted data – and a risk. What if you lose the key necessary to decrypt a critical piece of information? You may have backed up your data, but have you backed up your keys? Also, if using your key requires knowledge of a password, what if you forget the password?

The need to be careful with keys sounds obvious. However, perhaps less obvious is the need for the encryption software to be available to decrypt data when required. Of course, if encryption is used to protect transmitted data against eavesdropping, then it will typically be decrypted on receipt, in which case no long term storage of keys or availability of software is needed. However, if received encrypted data is retained in encrypted form then the same problems arise as when data is encrypted for long-term secure storage.

At first sight, non-availability of software does not sound very likely. If you have installed encryption software on your PC, then you might believe that there is no reason to expect it to stop working. However, I would suggest that this is dangerous complacency. I personally came across exactly this problem recently when upgrading my PC from Windows ME to XP. A few weeks after the upgrade, I had reason to use PGP to decrypt a file – I am not a major user of encryption, but I work on projects where encryption of exchanged data is mandated by the project manager. I immediately discovered major incompatibility problems between XP and PGP. Essentially, if you try and install a recent version of PGP on an XP system then there is a good chance that you will cause serious damage to your operating system. As I understand it, the installation has the side effect of corrupting your networking software – additionally, PGP will not work. In my case this meant several hours of increasing annoyance, culminating in a re-installation of XP (the ‘repair’ function does not seem to help).

From what I have gleaned from the Internet, if you use PGP and are about to upgrade to XP, then you should uninstall PGP first. After installing XP, you can re-install PGP, but you must either use an ‘old’ version of PGP (e.g. version 6.5.2a) or install a newer release in such a way that the particular features causing the problems are disabled. If you only need to use PGP to encrypt or decrypt files then the old version works fine – however, if you have an encrypted hard disk, or you are using some other feature only supported by more recent versions of XP, then you have a serious problem!

As I understand it, the present owners of PGP do not intend to continue supporting the product, and no XP-compatible version is even on the horizon. The main point in describing this issue is that the same problem could occur with any product. What would you do if the vendor of your encryption product decides to stop supporting it, or just goes out of business? Often, the old product will continue to work with newer versions of the operating system, but there is no guarantee of this.

What can we learn from the PGP/XP problems? Well I believe there are two very important lessons. First, I think that it is clear that there is little point in retaining files in encrypted form unless there is a good reason to do so. Unless you keep backup copies of the keys you need to decrypt the files concerned, it is analogous to not making back-ups of the data itself. Second, if you are a user of encryption, think very carefully before you upgrade your operating system. Unless you know that the encryption product you use works on the new operating system, it might be worth considering decrypting files before you upgrade, and re-encrypting them afterwards. This sounds like an awful pain, but not as unpleasant as some of the stories you can read on the web written by the many other PGP users who have upgraded to XP!